State of Maryland
State Data Security Committee Annual Report
January 2004

Introduction

In accordance with Executive Order 01.01.1983.18, Privacy and State Data System Security paragraph 4.E, the State Data Security Committee is pleased to submit the following annual report of activities for the calendar year 2003.

Membership

Members of the Committee during the 2003 calendar year were:

- Carmella Thompson for the Department of Budget and Management
- Kenneth Holloway for the Department of Public Safety and Correctional Services
- Joseph Distinti from the Department of Business and Economic Development
- John Sledgeski for the Department of Transportation
- David Bickel from the Department of Health and Mental Hygiene
- Sandra Johnson from the Maryland State Lottery
- Christian Granger for the University System of Maryland
- Donald Lee from the Department of Assessments and Taxation
- David Harrington for the Comptroller of Maryland

The membership of the Committee was changed with the departure of Joseph Distinti effective August 2003 and Donald Lee effective December 2003. This left two at large vacancies to be filled. The Committee is urging that these vacancies be filled as soon as possible. Selected Executive Branch agencies will be contacted to request nominations to the Committee.

Overview

The State Data Security Committee was created to regularly evaluate the security of state agency systems containing computerized records. The Committee consists of nine data professionals within State service. Each of the following agencies has a permanent representative on the Committee: Comptroller of the Treasury, Department of Transportation, Department of Public Safety and Correctional Services, the University of Maryland, the Board of Trustees of the State Universities and Colleges and the Department of Budget and Management, whose representative is the Chairman. The Governor upon the recommendation of the Chairman appoints the other members of the Committee. The Committee evaluates system risks including the review, formulation, and periodic testing of the appropriate levels of security. The Committee has no resources and relies on the resources provided by the Department of Budget and Management to assist in this evaluation.

Accomplishments

Review of Legislative Audit Reports

During calendar year 2003, the Committee reviewed the legislative audits for information technology (IT) security audit findings with special emphasis on repeated findings. There were no repeated information technology security findings requiring issuance of a follow-up letter from the Committee.

The reports reviewed were:

- The Department of Budget and Management/Central Collection Unit December 2002
- The University System of Maryland/Frostburg State University January 2003
- The Maryland State Lottery Agency December 2002
- The Department of Budget and Management/Financial Management Information System – Centralized Operations March 2003
- The Department of General Services – Office of Procurement and Contracting April 2003
- The Department of Labor, Licensing and Regulation Office of the Secretary May 2003
- The Maryland Aviation Administration June 2003
- The State Highway Administration June 2003
- The University of Maryland's Biotechnology Institute August 2003
- The Comptroller of Maryland's Central Payroll Bureau August 2003
- The Department of Juvenile Services September 2003
- The University of Maryland, College Park's Office of Information Technology September 2003
- The Department of Health and Mental Hygiene's Medical Care Programs Administration October 2003
- The University System of Maryland – University of Maryland Center for Environmental Science October 2003
- The Comptroller of Maryland's Revenue Administration Division November 2003
- The Maryland State Lottery Agency Follow-up Review November 2003
- The Executive Department November 2003

The most common IT security audit findings in the reports were:

1. Internal networks were not adequately secured from external threats
2. Insufficient disaster recovery plans
3. Proper physical access restrictions to facilities were inadequate
4. Inadequate monitoring of security events

The Information Technology Security Policy and Standards, which the Committee reviewed and discussed at several meetings prior to its release in June 2003, addressed these weaknesses.

Security Awareness Training

There were no security officer training courses scheduled in 2003. The Committee intends to resume this type of training in the future. The IT Security Awareness, Training and Education program being developed by the Department of Budget and Management, Office of Information Technology (DBM OIT) Security and Architecture Division would provide a base for all State employees. Only the first of the three levels of training has been completed in the newly developed program. A computer based training module will be developed for the first level training by the end of the second quarter 2004. This program will need to be expanded to include specific training for agency security officers.

Information Technology Security Policy and Standards

The Information Technology Security Policy and Standards was distributed in June of 2003.

Annual Information Technology Security Survey

The Committee voted to change the annual survey from a calendar year survey to a fiscal year. Therefore the Annual IT Security Survey, which has been expanded to be more consistent with the policy and standards, will be distributed in June 2004. Agencies will be required to complete the survey by July 31, 2004. It will be posted on the security web site for agencies to review prior to June 2004.

The survey has been modified to use a different format for responding to questions. The responses will be red, amber, or green with 'red' meaning an agency is not in alignment with the current policy and standards, 'amber' meaning the agency is currently making progress or is somewhat in alignment with the current policy and standards and green meaning an agency is compliant with the current policy and standards. Additional questions have been added to track specific metrics on key questions.

Information Technology Disaster Recovery

As stated in the semi-annual report, an audit was performed on the cold site at 301 West Preston Street Baltimore, Maryland. The results were positive and this site remains a viable solution for the mainframe data centers. Agencies received Information Technology Disaster Recovery Guidance documentation and training on this guidance during 2003 through the DBM OIT Security Division. Executive Branch agencies were requested by the DBM OIT Security Division to complete a "Quick Plan" if they had not completed their more formal disaster recovery plan. The "Quick Plan" included the following sections:

- Definition of what constitutes a disaster. (Narrative description)
- Creation of an Emergency Notification Contact List (Email, Home, Cell, pager, fax numbers).
    - Statewide Contact Info
    - Agency Customer Info
    - Agency Vendor Info (critical components & supplies)
    - Agency Senior Staff Info
    - Agency Incident Response Team Info
- Ensuring that backups of all critical information are stored securely at an offsite location. (*Offsite contact information should also be included in the Emergency Notification List*)
- Establish an inventory of critical IT systems, which should include:
- All associated hardware, software, and licenses (copies should reside offsite), necessary to support them
- Outlining of the general steps to recover critical IT operations. This would include the restoration steps, configuration requirements, and technical considerations

2003 IT Security and Privacy Conference

The Committee reviewed and supported The Department of Budget and Management sponsored 2003 State of Maryland IT Security and Privacy Conference held on September 24th and 25th 2003, at Camp Fretterd, Reisterstown. More than 200 participants received timely information on IT Security topics during this two-day conference. Information on the conference and presentations received at the conference can be found at *http://www.dbm.maryland.gov/DBM_Search/Security/tocITSecurityConferenceSept2003.html.*

Information Technology Security Incidents

In the first quarter of CY2003, all Executive Branch agencies were given guidance documents for reporting incidents to the DBM OIT Security Division. The security incidents in the State Data Security Committee Report will be by fiscal year to remain in alignment with the annual surveys and the State's Managing For Results program. During FY2003, only one major incident was reported.

2003 Meetings Held

February 21, 2003 at 9:30 AM	Maryland Department of Transportation
April 25, 2003 at 9:30 AM	Comptroller of Maryland
June 26, 2003 at 9:30 AM	Department of Assessments & Taxation
August 21, 2003 at 9:30 AM	Department of Budget and Management
October 23, 2003 at 9:30 AM	Maryland State Lottery
December 11, 2003 at 9:30 AM	Department of Health and Mental Hygiene

Schedule of Meetings and Activities for 2004

January	2004	CY 2003 Annual Report
February	2004	Meeting at the Maryland Department of Transportation
April	2004	Meeting Department of Budget and Management
May	2004	Plan for Fall Conference
June	2004	FY 2004 Data Security Surveys Distributed.
June	2004	Meeting Maryland State Lottery
July	2004	CY 2004 Semi-Annual Report due
July	2004	Agency Data Security Surveys due
August	2004	Meeting Comptroller of Maryland
September	2004	Annual Security Conference
October	2004	Meeting Department of Public Safety and Correctional Services
December	2004	Meeting University of Maryland

Submitted by:

Carmella F. Thompson________________________
Name

Chairman, State Data Security Committee________
Title

March 1, 2004________________________________
Date